

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平8-340331

(43) 公開日 平成8年(1996)12月24日

(51) Int.Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
H 0 4 L 9/32			H 0 4 L 9/00	6 7 3 B
G 0 6 F 15/00	3 3 0	9364-5L	G 0 6 F 15/00	3 3 0 C
G 0 9 C 1/00	6 4 0	7259-5J	G 0 9 C 1/00	6 4 0
			H 0 4 L 9/00	6 7 3 C

審査請求 未請求 請求項の数7 O L (全 9 頁)

(21) 出願番号 特願平8-131694

(22) 出願日 平成8年(1996)5月27日

(31) 優先権主張番号 4 5 5 6 1 4

(32) 優先日 1995年5月31日

(33) 優先権主張国 米国 (U S)

(71) 出願人 390035493

エイ・ティ・アンド・ティ・コーポレーション

AT&T CORP.

アメリカ合衆国 10013-2412 ニューヨーク ニューヨーク アヴェニュー オブジ アメリカズ 32

(72) 発明者 マイラ エル. エンサー

アメリカ合衆国, 07901 ニュージャージー, サミット, ピーチ スプリング ドライブ 3シー

(74) 代理人 弁理士 三俣 弘文

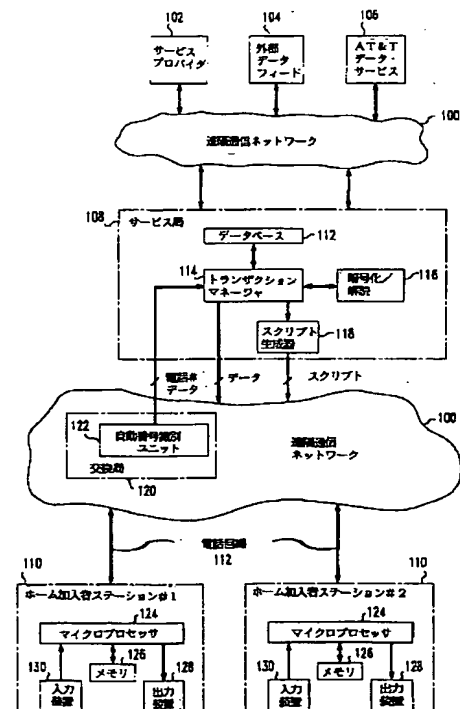
最終頁に続く

(54) 【発明の名称】 ネットワークへのユーザ端末のアクセスを認証するための方法および装置

(57) 【要約】

【課題】 複数の加入者ステーション110が通信可能に結合されたネットワーク100のためのパスワード認証セキュリティシステムを提供する。

【解決手段】 加入者ステーション110との通信の確立により、加入者ステーションが結合されている回線の電話番号を含むネットワーク結合識別子が、電話交換局120において検出され、制御センター108に送信される。1回目に通信が確立された場合、受信された電話番号は、秘密のパスワードを生成するために暗号化され、メモリ126に記憶させるために、加入者ステーション110に自動的に送信される。その後の通信において、電話番号が制御センター108により再度受信され、暗号化され、第2のパスワードが生成される。第1のパスワードが、ユーザとのかかわり合いと独立に、メモリ126から自動的に検索される。2つのパスワードが比較され、少なくとも類似している場合、制御センターが、加入者ステーションからの呼びをネットワークのサービスプロバイダ102、データベース104、106などに結合する。



【特許請求の範囲】

【請求項1】 有線ネットワーク、無線ネットワーク、衛星ネットワーク、ファイバ光ケーブルネットワーク、および同軸ケーブルネットワークのうちの1つからなる遠隔通信ネットワーク（100）への、このネットワークと通信可能に結合された複数のユーザ端末（110）のうちの選択された1つからのアクセスに権限が与えられているかどうかを決定するための方法において、選択されたユーザ端末から前記ネットワークへ入ってくる呼びの受信により、選択されたユーザ端末のネットワーク結合識別子を検出するステップと、前記ユーザ端末からパスワードを受信するステップと、前記識別子とパスワードを比較するステップと、前記識別子の少なくとも一部が前記パスワードの少なくとも一部と一致する場合、前記ネットワークへのアクセスを前記選択されたユーザ端末に対して許可するステップと、前記識別子および前記パスワードに一致する部分がない場合、前記ネットワークへのアクセスを前記選択されたユーザ端末に対して拒否するステップとを有し、前記識別子が、選択されたユーザ端末から入ってくる呼びにより使用される前記ネットワークの通信チャネル（112）に関する情報を含むことを特徴とするネットワークへのユーザ端末のアクセスを認証するための方法。

【請求項2】 前記ネットワークが、前記ネットワークと通信可能に結合された、複数のユーザ端末から入ってくる呼びを受信するためのネットワークサービスセンターを有する電話ネットワークからなり、ネットワーク結合識別子を検出するステップが、電話ネットワーク交換局の自動番号識別ユニットから、選択されたユーザ端末の入ってくる呼びに結び付けられた電話番号を受信するステップであることを特徴とする請求項1記載の方法。

【請求項3】 ネットワークへのアクセスを許可するステップおよびネットワークへのアクセスを拒否するステップが、識別子およびパスワードの少なくとも一部が一致する場合、選択されたユーザ端末の入ってくる呼びを、ネットワークサービス、ネットワークデータベース、およびネットワーク出力装置のうちの1つに結合するステップと、識別子およびパスワードの少なくとも一部が一致しない場合、選択されたユーザ端末の入ってくる呼びを、ネットワークから切り離すステップであることを特徴とする請求項2記載の方法。

【請求項4】 ネットワークとユーザ端末との間に最初の通信が確立した場合に、第1の暗号化されたパスワードを生成するために、識別子を暗号化するステップと、

前記ユーザ端末のメモリ中に記憶させるために、前記ネットワークを介して前記ユーザ端末へ前記第1の暗号化されたパスワードを送信するステップとをさらに有することを特徴とする請求項1記載の方法。

【請求項5】 識別子およびパスワードを比較するステップが、ユーザ端末から受信された第1の暗号化されたパスワードとの比較のために、第2の暗号化されたパスワードを生成するために識別子を暗号化するステップと、検出された識別子との比較のために、解読された識別子を生成するために第1の暗号化されたパスワードを解読するステップとからなるステップから選択されたステップをさらに有することを特徴とする請求項1記載の方法。

【請求項6】 ネットワークに結合された複数のユーザ端末のうちの選択された1つからの前記ネットワークへのアクセスを認証するためのセキュリティシステムにおける、前記ネットワークへのアクセスを得るために使用されるパスワードを選択し、前記選択されたユーザ端末に渡すための方法において、

ネットワークとユーザ端末との間の通信の確立に応じて、選択されたユーザ端末の通信チャネルおよびネットワークアドレスのうちの1つを検出するステップと、秘密のパスワードを生成するために前記識別子を暗号化するステップと、

前記ネットワークを介して、ユーザ端末へパスワードを送信するステップとを有し、

前記識別子が、ネットワークへのユーザ端末の結合の固有の情報を含むことを特徴とするネットワークへのユーザ端末のアクセスを認証するための方法。

【請求項7】 ネットワーク（100）に通信可能に結合された複数のユーザ端末（110）を有する遠隔通信ネットワークのためのセキュリティシステムにおける、メモリ（126）を有する複数のユーザ端末のうちの選択された1つからネットワークへのアクセスを認証するための装置において、

ネットワークとユーザ端末との間の通信の確立に応じて、ネットワークに通信可能に結合された、選択されたユーザ端末のメモリからネットワーク結合識別子を受信するためのネットワークサービスセンター（108）を有し、

このネットワークサービスセンターが、前記識別子と、選択されたユーザ端末のメモリ中の所定のロケーションから読み込んだパスワードとを比較するための比較ロジックと、

前記比較結果に基づいて、選択されたユーザ端末がネットワークへのアクセスを許可または拒否するためのスイッチとを含み、

識別子は、選択されたユーザ端末から入ってくる通信の通信チャネルインジケータ、ネットワークアドレス、および電話番号のうちの1つを含むことを特徴とするネッ

トワークへのユーザ端末のアクセスを認証するための装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータネットワークおよび遠隔通信ネットワークの両者において使用されるパスワード認証セキュリティシステムに関する。

【0002】

【従来技術の説明】ネットワークセキュリティは、ネットワークおよびネットワーク利用における最近の急増とともに、ますます問題となってきた。よりユーザフレンドリーなネットワークプラットフォームの出現および無数のオンラインデータベースおよびサービスへの容易なアクセスによって、伝統的な形のネットワークセキュリティは、権限を与えられたユーザまたは支払っている加入者のみが守られたネットワークへのアクセスを得ることを可能にすることを保証するにはもはや十分ではなくなっている。

【0003】UNIX™に基づくシステムのような典型的なコンピュータネットワークにおいて、セキュリティは、ユーザログインおよび秘密のパスワードにより、各ユーザとセキュリティチェックを実行するネットワークサーバとの間で遂行される。最初のアクセスにより、ユーザは、ネットワーク上の彼のアドレスとして使用されるべきログインと、認証のチェックに使用するための秘密のパスワードを選択する。ユーザは、これらの選択をネットワークサーバに送信し、秘密のパスワードは、暗号化されたデータベースすなわち彼のログインに結び付けられたディレクトリに格納される。

【0004】その後のネットワークへの接続において、ユーザは、彼のログインおよび彼の秘密のパスワードの両者を質問される。サーバは、彼のログインを使用して、格納されたパスワードを検索し、それをユーザにより現在与えられているパスワードと比較する。認証チェックが実行され、両方のパスワードが同じ場合に、ユーザがネットワークへアクセスすることが許可される。

【0005】

【発明が解決しようとする課題】しかし、この形のパスワードセキュリティは、ユーザのかかわり合い依存する問題に悩まされている。ユーザは、まず、パスワードの選択または同意をすることを求められ、次に、パスワードを記憶し、ネットワークへアクセスすることを望むたびにサーバにパスワードを与えることを求められる。このようにする場合、多くのユーザは、パスワードを忘れないように書きとめてあり、さらに、パスワードの入力を他人に知られないように実行することを必ずしもいない。

【0006】従って、セキュリティが、ネットワークに対して形成される特定の接続ではなく特定のユーザの

パスワードに依存しているので、この権限が与えられていないアクセスは、ネットワークに接続されているどの端末からでも実行可能である。

【0007】ネットワークユーザが、ホームバンキングおよびホームショッピングのような金融および消費者サービスに対する数百万人のネットワークユーザのうちの1人となる未来の世界において、このセキュリティシステムが被害を受けやすいことは、さらに重大な事柄となる。数百万人の加入者それぞれについての加入者の財政の安全が各加入者の適切な行為に依存する場合、パスワードの秘密を維持する上で適切な手段をとらない加入者を容易にだます犯罪的構成要素が確かにある。また、選択されたパスワードは端末を特定するものではなく、ユーザを特定するものなので、加入者への口座またはサービスへの権限が与えられていないアクセスは、事実上知られることなく行うことができる。これは、違反者が特定の端末からアクセスを行うように制限されないからである。

【0008】本発明の1つの目的は、ネットワークユーザまたは加入者に独立かつトランスペアレントなコンピュータネットワークまたは遠隔通信ネットワークのいずれかにおいてセキュリティを遂行するための方法および装置を提供することである。

【0009】本発明の他の1つの目的は、ユーザまたは加入者によりなされるネットワークへの特定の接続を識別するパスワードの認証に基づいて、ネットワークのサービス、データベースまたは装置へのアクセスを安全にするための方法および装置を提供することである。

【0010】本発明のさらなる他の1つの目的は、ネットワークの自動番号識別サービスを使用することにより、パスワードが最初に生成され、その後、ネットワーク制御センターにより自動的に認証される、電話ネットワークへのアクセスを安全にするためのパスワードセキュリティシステムを提供することである。

【0011】

【課題を解決するための手段】本発明は、自動的に決定されるネットワーク結合識別子および自動的に受信される暗号化されたパスワードに基づく、遠隔通信ネットワークまたはコンピュータネットワークのサービス、データベースまたは装置へのアクセスを安全にするための方法および装置を提供する。ユーザ端末または加入者ステーションからネットワークへアクセスがなされる場合、ネットワーク上でセキュリティシステムを具現化するネットワーク制御センターは、ネットワークへの結合を特定するユーザ端末の固有のネットワーク結合識別子を、ネットワークから受信する。

【0012】本発明の一実施形態において、ネットワークは、電話ネットワークであり、識別子は、ユーザ端末をネットワークへ結合する特定の電話回線の電話番号およびネットワークの自動番号識別サービスにより決定さ

れる番号で形成される。他の一実施形態において、ネットワークは、コンピュータネットワークであり、識別子は、特定の端末のネットワークアドレス、サーバ、またはユーザディレクトリで形成される。

【0013】ネットワークへのユーザ端末の識別された結合により、ネットワークへの1回目のアクセスがなされた場合、ネットワーク制御センターは、秘密の暗号化されたパスワードを得るために、ネットワーク結合子を検出し、選択し、ネットワークに内在する暗号化キーを使用して暗号化する。そして、パスワードは、ユーザに知られないように、ユーザ端末のメモリ中にダウンロードされる。

【0014】その後のユーザ端末によるネットワークへの各接続において、制御センターは、加入者の現在検出されているネットワーク結合識別子および同じネットワーク暗号化キーを使用して、もう1つの暗号化されたパスワードを生成する。次に、制御センターは、ユーザ端末のメモリに以前に格納された暗号化されたパスワードをアップロードし、この2つのパスワードを比較する。これらが一致する場合、これは、同じユーザ端末が同じネットワーク接続からアクセスを要求していることを意味し、いかなるユーザの干渉とも独立にセキュリティが維持される。2つのパスワードが一致しない場合、ユーザに問題が通知され、パスワードまたはネットワークへのユーザ端末の結合のいずれかが偽造されたとみなして、ネットワーク接続がネットワーク制御センターにより終了される。

【0015】

【発明の実施の形態】本発明は、複数のユーザ端末110、202を有するネットワーク100、200のためのパスワード認証セキュリティシステムを提供する。複数のユーザ端末110、202は、ネットワーク100、200と通信できるように結合されている。図1および図2にそれぞれ示されているように、システムは、ネットワーク制御センター108、206をそれぞれ有する遠隔通信ネットワーク100またはコンピュータネットワーク200のいずれかにおいて具現化することができる。

【0016】ネットワーク制御センター108、206は、ユーザ端末110、202によるネットワーク110、200へのアクセスおよび通信を監視および/または処理するために、ネットワーク100、200に結合されている。ユーザ端末110、202は、割り当てられたデータ通信チャネル、ネットワークノードまたは遠隔端末リンクのアドレス、または電話ネットワークの電話回線のような固有に識別可能なネットワーク結合112、212を介して、ネットワーク100、200へ結合されている。

【0017】図2に示されたコンピュータネットワーク200において、ネットワーク制御センターは、ネット

ワークサーバ206および結び付けられたネットワークデータベース208からなる。ネットワークサーバ206および結び付けられたネットワークデータベース208は、LANまたはWANのようなコンピュータネットワーク200を介して複数のユーザ端末202およびネットワーク出力装置204に結合されている。コンピュータネットワーク200へのアクセスは、典型的には、図示されていないネットワークサーバのアクセス制御ユニットにより監視され、実行される。

【0018】コンピュータネットワーク200への接続がユーザにより要求された場合、アクセス制御ユニットは、ユーザ端末202のネットワークアドレスすなわちロケーションを認知する。このロケーションは、そのローカルネットワークサーバアドレス、サブネットへの遠隔リンクアドレス、およびユーザの割り当てられたネットワークディレクトリを含み得る。制御ユニットは、ネットワークサーバ206への接続スロットの利用可能性を決定し、ユーザがネットワーク出力装置204および/またはネットワークデータベース208をアクセスするための権限を有するかどうかを決定する。

【0019】図1において、有線ネットワーク、無線ネットワーク、衛星ネットワーク、ファイバ光ケーブルネットワーク、同軸ケーブルネットワークなどのような遠隔通信ネットワーク100は、ネットワークサービス局を形成するネットワーク制御センター108を有するものとして示されている。ネットワークサービス局（ネットワーク制御センター）108は、ホームまたはビジネス加入者ステーションを形成する複数のユーザ端末110に結合されており、遠隔通信ネットワーク100を介して、サービスプロバイダ・ステーション102、外部データフィード104、および外部データベース106に結合されている。

【0020】この実施形態において、ネットワークサービス局108は、サービスプロバイダ・ステーション102からのオンラインサービスと外部データフィード104および外部データベース106からのデータとをホームおよびビジネス加入者ステーション110中の端末装置へ与えるための中間的送信ステーションとして働く。これを達成するために、ネットワークサービス局108は、ネットワーク接続、ネットワークパスワード認証、加入者ステーション110へのデータ通信およびスク립ト・メッセージングを処理するために、トランザクション・マネージャのようなマイクロプロセッサ・ロジック114、内部データベース112、およびスク립ト生成器118を含む。

【0021】また、ネットワークサービス局108は、新たなハードウェア特徴および/またはサービスを具現化するために端末ソフトウェアをアップグレードするために、および端末に内在する新たなソフトウェアアプリケーションを提供するために、加入者ステーション11

0の端末へのソフトウェアのダウンロードを可能にする。以下に説明する加入者装置の実施形態において、端末に内在する特定のソフトウェアが、端末に直接またはホームネットワークを介して結合され得る他の装置の動作を制御および処理するために、ライセンスされ、かつネットワークサービス局108から端末へダウンロードされ得る。

【0022】そのような用途における本発明の1つの利点は、加入者端末を有するが特定のサービスについて登録されていないユーザが、他の登録されたユーザのネットワーク接続（すなわち、電話回線）を介して、登録されたユーザのネットワーク接続へ自分の端末を接続することにより、ソフトウェアを不正にダウンロードすることを防止することである。一度ダウンロードされたソフトウェアの不正な複製行為は、加入者端末が、コンピュータシステムである必要はないという事実により、ソフトウェアがそれによって複製される代替的入出力装置（すなわちフロッピー・ドライブ）を有さないようにすることにより禁止される。

【0023】加入者ステーション110は、実際に、通常の方法により遠隔通信ネットワーク100に接続されるように適合された、データの処理およびネットワークトランザクションの処理のためのマイクロプロセッサ124と、図示しないデータを送受信するトランシーバと、非持久性および／または持久性のデータ記憶のためのメモリ126と、ユーザからの入力を直接受け取るユーザ入力装置（すなわち、キーボード、マウス、リモコンなど）130と、メッセージおよびデータをユーザに対して表示するためのユーザ出力装置（すなわち、ディスプレイ、オーディオスピーカなど）128とを有する。いかなる端末装置も含むことができる。このような端末装置（加入者ステーション）110は、電話ハンドセット、電話応答システム、およびコンピュータシステムを含み、これらに限定されない。

【0024】図示されていないホーム加入者ステーションのための端末装置110の特定の例において、ホーム電話応答システムは、標準的オーディオ／ビデオ入出力を介してテレビジョンに結合され、標準的RF入出力を介してケーブルチャネルチューナーに結合され、標準的RJ11電話ジャックを介して電話ネットワークに結合される。

【0025】このシステムは、入力装置としてのリモコン、出力装置としてのテレビジョンディスプレイモニタを有し、さらに、ネットワークトランザクションの処理およびデータの処理のためのメモリを有するマイクロプロセッサと、入ってくる呼びおよび出ていく呼びを処理するための呼び信号演算処理ユニットと、デジタル信号を処理し、DTMFトーンを検出し、マイクロプロセッサへ情報を通知し、デジタル応答マシンおよびデータモデムを具現化するために呼び信号演算処理ユニットと相

互作用するデジタル信号演算処理ユニットと、リモコン、ケーブルチャネルチューナー、およびテレビジョンモニタの間で信号を受信し、処理し、送信するためのビデオ変調器／エンコーダユニットを含む。

【0026】上述の実施形態において、加入者とネットワークサービス局108との間の典型的なトランザクションは、加入者ステーションの端末装置110にネットワークサービス局108への通話を開始するように指示する加入者からなる。これは、ユーザ端末を立ち上げて、端末ディスプレイ128上に生成されるメニュー選択から「オンラインサービス」オプションおよび「ソフトウェアダウンロード」オプションのうちの1つを選ぶことにより達成される。次にユーザ端末は、ネットワークサービス局108へのモデム通話を開始し、モデムハンドシェイクが完了した後、自動ユーザトランスペアレント認証ハンドシェイクが開始される。

【0027】図3のフローチャートに示されているように、認証ハンドシェイクは、サービス局トランザクションマネージャ114（図1）により、ネットワークサービス局108によりユーザ端末へのアクセスを得ようとする特定のユーザ端末110のための固有のネットワーク結合識別子を遠隔通信ネットワーク100からまず受信することにより実行される。通常の電話ネットワーク（遠隔通信ネットワーク）100の場合、この識別子は、ユーザ端末110を遠隔通信ネットワーク100に結合する専用の電話回線に結び付けられた電話番号からなる。

【0028】この電話番号は、例えば、接続された電話ネットワーク交換局120内で使用される自動番号識別ユニットすなわちサービス122による番号の検出により、通常の方法で得られる。しかし、なんらかの理由で、自動番号識別サービス122が端末の電話番号を提供しない場合、サービス局トランザクションマネージャ114は、結び付けられた入力装置130の使用により電話番号を直接提供するように加入者に要求するユーザ端末110へ、スクリプトメッセージをダウンロードする。

【0029】特定のユーザ端末110の電話番号が受信されると、サービス局トランザクションマネージャ114は、この番号をネットワークサービス局108の暗号化／解読ユニット116へ送る。この番号は、図示しない通常の暗号生成器を使用して暗号化され、秘密の暗号化されたパスワードが生成される。次に、サービス局トランザクションマネージャ114は、そのロケーションに以前に格納されたであろうパスワードをメモリ126の所定のロケーションから検索することを、ユーザ端末110の端末マイクロプロセッサ124に要求する。

【0030】このメモリロケーションにパスワードが発見されなかった場合、端末マイクロプロセッサ124は、この状態をサービス局トランザクションマネージャ

114に通知し、サービス局トランザクションマネージャ114は、特定のユーザ端末110がすでにネットワークサービス局108により登録されているかどうかを決定するために、ネットワークサービス局の内部データベース112に質問する。これは、暗号化されたパスワードを、ネットワークサービス局の内部データベース112に格納された全てのユーザ端末110の登録された口座を識別するために使用される暗号化されたパスワードのリストと比較することにより行われる。

【0031】この比較において、暗号化されたパスワード間の一致が見いだされなかった場合、これは、ユーザ端末110が以前に登録されていなかったことを意味する。従って、サービス局トランザクションマネージャ114は、新たに暗号化されたパスワードにより識別された内部データベース112中に加入者登録口座をつくることにより、この特定のユーザ端末を登録する。また、114は、新たに暗号化されたパスワードをメモリ126の所定のロケーションに記憶させるためにユーザ端末110に送信する。その後の認証ハンドシェイクにより、ユーザ端末110は、以前に登録されていたと決定されることになる。

【0032】最後に、ネットワークサービス局108は、要求されたソフトウェアをユーザ端末110にダウンロードすることにより、またはユーザ端末110をサービスプロバイダ102に結合することにより、トランザクションを続ける。サービスプロバイダ102への結合は、入ってくる呼びをサービスプロバイダ102に送る（または、リレーする）こと、またはサービスプロバイダの電話番号をユーザ端末に提供することのいずれかにより、実行される。そして、その後の呼びにより、直接的な接続が形成できるようになる。

【0033】しかし、新たに暗号化されたパスワードと暗号化されたパスワードのデータベースリストとが一致する場合、これは、端末のメモリ126中にあったはずのパスワードが偽造されたか、またはメモリ126からのパスワードの読みだしあるいはネットワークサービス局108へのパスワードの送信においてハードウェア故障があったかのいずれかを意味する。いずれの場合にも、エラーメッセージは端末の出力装置128に送られて、表示され、加入者に問題を通知し、この問題を解決するためにネットワークサービス局108への音声通話を行うよう加入者に指示する。そして、サービス局トランザクションマネージャ114は、加入者を遠隔通信ネットワーク100から分離するために、モデム接続を終了させるよう遠隔通信ネットワーク100に指示する。

【0034】メモリ126中の所定のロケーション中に格納されたパスワードを検索するためのユーザ端末110へのトランザクションマネージャの要求がパスワードを返す場合、これは、ユーザ端末110が以前のトランザクションにおいてすでに登録されていたことを意味す

る。この場合、サービス局トランザクションマネージャ114は、新たに暗号化されたパスワードを認証目的のために検索されたパスワードと比較する。

【0035】2つのパスワードが同一でない場合、エラーメッセージがユーザ端末110に送られ、端末のメモリ126に格納されたパスワードの偽造、ハードウェア故障、または特定のユーザ端末と専用の電話回線112との間のミスマッチのために、認証が失敗したことを加入者に対して表示する。再び、加入者は、問題を解決するためにネットワークサービス局108への音声通話をなすように指示され、モデム接続は終了される。

【0036】2つのパスワードが同一であると決定された場合、認証ハンドシェイクは成功して、ネットワークサービス局108は、要求されたソフトウェアをユーザ端末にダウンロードすること、またはユーザ端末110を102に結合することにより、トランザクションを続ける。ネットワーク100、200へのアクセスを許可するかどうかを決定するために、パスワードの一致についての比較を実行することが好ましいが、パスワードが単に類似している場合、またはパスワードの一部のみが実際に一致している場合に、アクセスが許可されるパスワード比較を実行することも有利である。

【0037】これは、例えば、ネットワークユーザの所定のグループ内の各ユーザへのアクセスを許可することが望ましい場合に有利となる。従って、コンピュータネットワーク200について、これは、各ユーザのネットワークアドレスがサブネットワークを特定するという事実によって、所定のサブネットワーク上の全てのユーザがコンピュータネットワーク200へのアクセスを得ることを可能にする。電話ネットワーク100について、これは同様に、各加入者についての電話番号が同じ地理的トランク番号を含むという事実によって、特定の交換局によりサービスされる所定の地理的領域内の全ての加入者が電話ネットワーク100へのアクセスを得ることを可能にする。

【0038】また、ユーザ端末110、202のメモリ126内に格納されたパスワードを自動的に変更すること、および制御センターの内部データベース112、208中に格納されたパスワードの対応するリストを更新することのために、ネットワーク制御センター108、206においてプロセスを遂行することにより、この自動的ユーザトランスベアレント・パスワード認証システムをより信頼できるものとするができることが予知される。これは、ネットワーク制御センター108、206により生成された異なる暗号化キーを使用してネットワーク結合識別子を暗号化することにより、選択されたユーザ端末110、202についての最初のパスワード認証の後に実行されることになる。

【0039】ネットワーク制御センター108、206は、それ自体の内部データベース112、208および

ユーザ端末 110、202 の所定の（または代替りの）メモリロケーション 126 のそれぞれの中のオリジナルのパスワードをユーザの知識なしに自動的に置き換える。また、識別子が暗号化される場合、満了日をパスワードに追加し、ユーザがネットワークおよび／または特定のサービスに現在登録されているかどうかをサービスプロバイダに通知することができる。

【0040】ここに記載された実施形態は、本発明の原理を開示するものであるが、これらの実施形態は、単なる例示であり、本発明の精神および範囲から離れることのない様々な付加および修正があり得る。例えば、ネットワークから加入者へのサービスおよび情報の提供のためのネットワークサービス局での加入者のトランザクションのシナリオにおいて、本発明は、ネットワークにより加入者の電話に割り当てられた電話番号を介して、サービス局において維持されている加入者口座をもつ加入者を固有に識別するために使用できる。加入者を異なる所在すなわち加入者ステーションに再割り当てすることができるが、加入者の古い電話番号の新しい加入者ステーションへの再割当は、サービス局が、再割当にもかかわらず、以前の口座との加入者の関連性を維持することを可能にする。

【0041】

【発明の効果】以上述べたように、本発明によれば、ネットワークユーザまたは加入者に独立かつトランスペアレントなコンピュータネットワークまたは遠隔通信ネットワークにおいてセキュリティを遂行するための方法および装置を提供することができる。

【図面の簡単な説明】

【図1】 複数の加入者ステーションがネットワークサービス局、複数のサービスプロバイダステーション、および複数のデータフィードおよびデータベースのそれぞれに結合される本発明の一実施形態による遠隔通信ネットワークを示すブロック図。

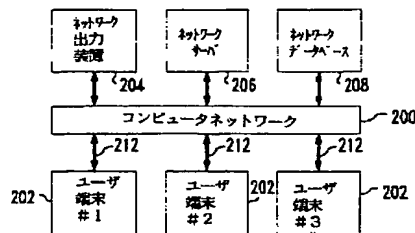
【図2】 複数のユーザ端末がネットワークサーバ、ネットワークデータベース、およびネットワーク出力装置に結合される本発明の一実施形態によるコンピュータネットワークを示すブロック図。

【図3】 本発明の一実施形態による遠隔通信ネットワークにおいて遂行されるパスワード認証プロセスを示すフローチャート。

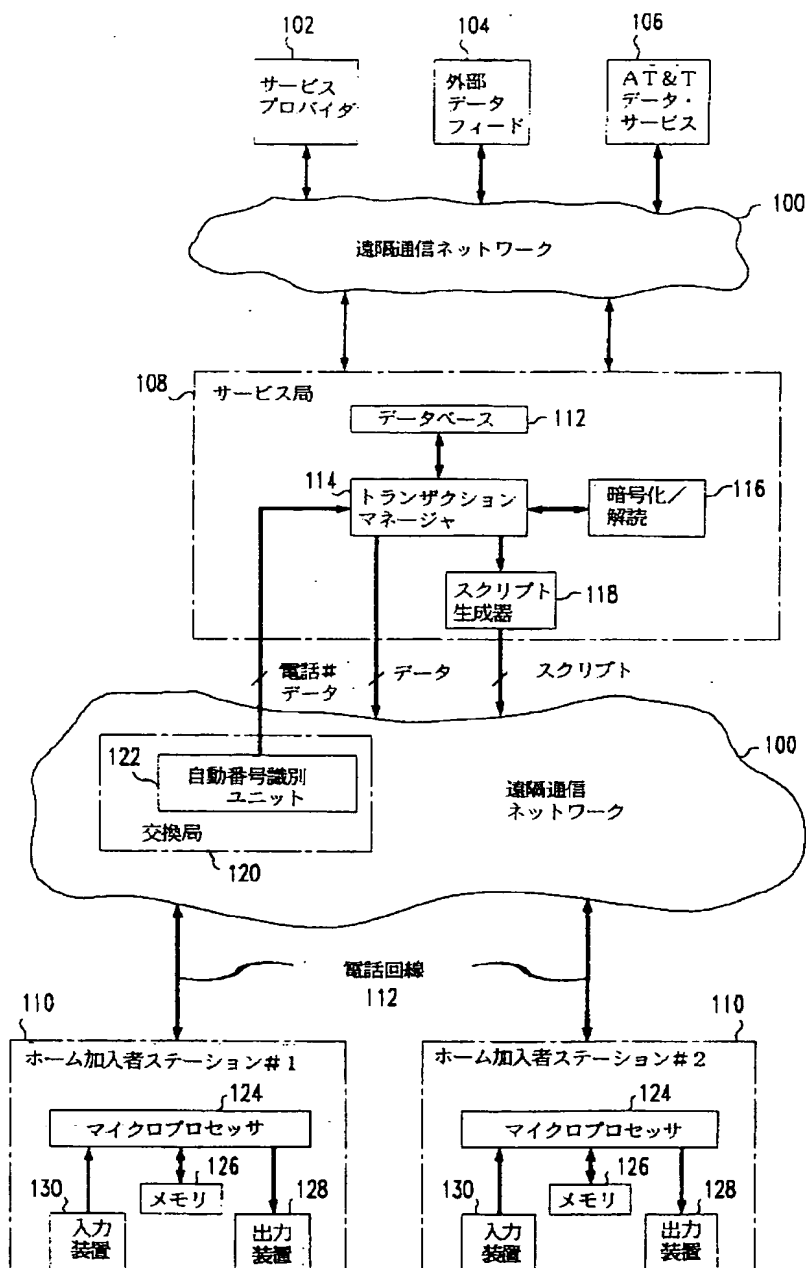
【符号の説明】

100	遠隔通信ネットワーク
102	サービスプロバイダステーション
104	外部データフィード
106	外部データベース
108	ネットワーク制御センター（サービス局）
110	加入者ステーション
112	電話回線
114	トランザクションマネージャ
116	暗号化／解読ユニット
118	スクリプト生成器
120	電話ネットワーク交換局
122	自動番号識別ユニット
124	マイクロプロセッサ
126	メモリ
128	出力装置
130	入力装置

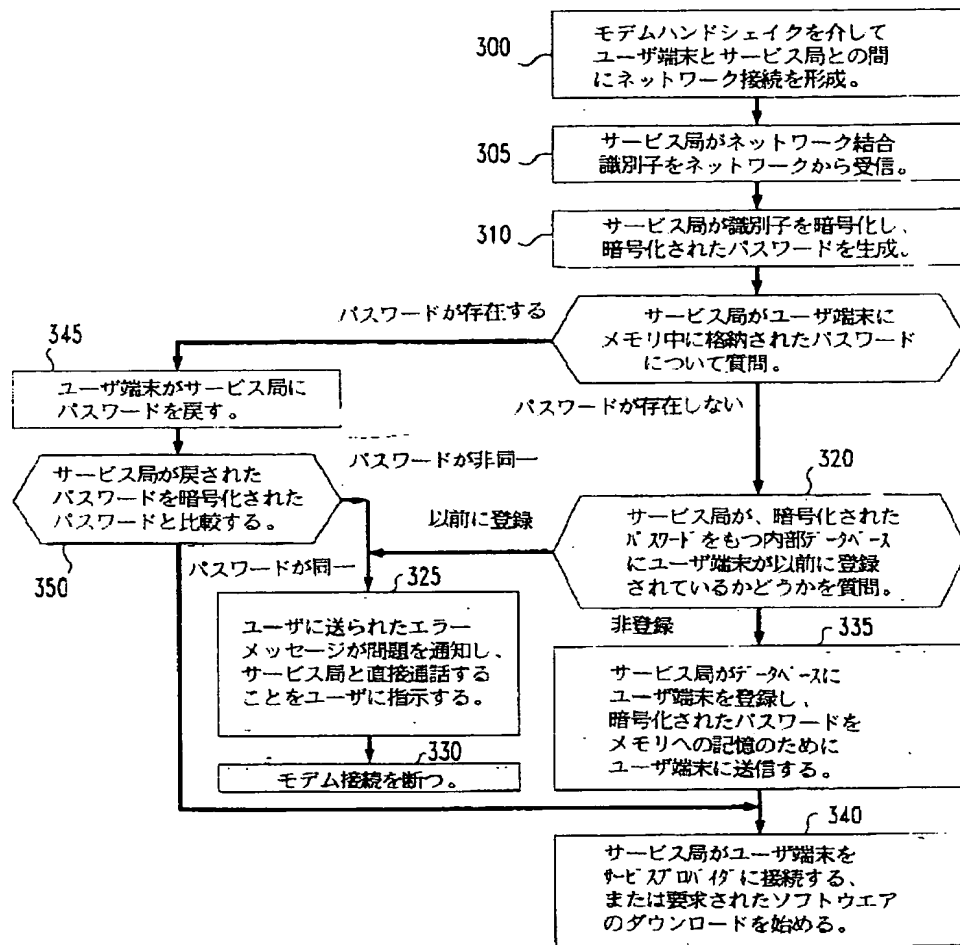
【図2】



【図 1】



【図 3】



フロントページの続き

(72)発明者 タッデウス ジュリアス コワルスキー
 アメリカ合衆国, 07901 ニュージャージー
 ー, サミット, ストーンリッジ ロード
 73

(72)発明者 アジェシノ プリマティック
 アメリカ合衆国, 08825 ニュージャージー
 ー, フレンチタウン, ワゴン ホイール
 ドライブ 4

拒絶理由通知書

11 8 K Y

特許出願の番号	特願 2 0 0 1 - 1 7 6 4 1 8
起案日	平成 1 7 年 8 月 4 日
特許庁審査官	高橋 宣博 9 3 7 4 5 J 0 0
特許出願人代理人	岡部 正夫 (外 1 0 名) 様
適用条文	第 2 9 条第 2 項

この出願は、次の理由によって拒絶をすべきものである。これについて意見があれば、この通知書の発送の日から 3 か月以内に意見書を提出して下さい。

理 由



この出願の下記の請求項に係る発明は、その出願前日本国内又は外国において頒布された下記 of 刊行物に記載された発明又は電気通信回線を通じて公衆に利用可能となった発明に基いて、その出願前にその発明の属する技術の分野における通常の知識を有する者が容易に発明をすることができたものであるから、特許法第 2 9 条第 2 項の規定により特許を受けることができない。

記 (引用文献等については引用文献等一覧参照)

- ・ 請求項 1 - 1 2
- ・ 引用文献等 1 - 3
- ・ 備考

1. 引用文献の記載事項

(1) 引用文献 1

「If the time run out, i.e. if the mobile terminal cannot authenticate itself at the access node within the predefined time period, then the already setup wireless ATM radio communication connection is interrupted (closed) and information regarding the mobile terminal (which has unsuccessfully attempted an authentication) is stored is the access node . Preferably, if the same mobile terminal has already failed an authentication a predetermined number of times, then further access requests from this mobile terminal are immediately rejected by the access node.」 (第 1 2 頁) と記載されており、認証失敗という結果になるときには、移動体ユニットのネットワークへのアクセスを拒絶する技術が示されている。

(2) 引用文献2

「【0035】2つのパスワードが同一でない場合、エラーメッセージがユーザ端末110に送られ、端末のメモリ126に格納されたパスワードの偽造、ハードウェア故障、または特定のユーザ端末と専用の電話回線112との間のミスマッチのために、認証が失敗したことを加入者に対して表示する。再び、加入者は、問題を解決するためにネットワークサービス局108への音声通話をなすように指示され、モデム接続は終了される。」と記載されており、認証が失敗した時にアナウンスメントを移動体ユニットに提供する技術（エラーメッセージがユーザ端末110に送られ）、及び、顧客サービスセンターに連絡する技術が示されている。

(3) 引用文献3

「【0005】

【発明が解決しようとする課題】ところで、上述した従来の電話端末装置では、メールの授受を行うために、サービスセンタへの発呼のための操作が必要となる。例えば、通信相手が発呼に応答しなかった場合、その発呼元の電話端末装置では、一旦通信相手への発呼を終了した後、改めてサービスセンタに対する発呼を行わなければならない。つまり、発呼元の電話端末装置のユーザは、一旦発呼を終了するための操作と新たな発呼のための操作とを行う必要があり、そのために煩わしさを感じてしまう可能性がある。

【0006】これに対して、周知の転送技術（転送電話サービス）等を利用して、通信相手への発呼をサービスセンタへの発呼に自動的に切り替えることも考えられる。」と記載されており、電話が繋がらない場合に、別の場所へ自動的にルーティングする技術が示されている。

2. 判断

引用文献2に記載された認証失敗時の技術を引用文献1に適用することは当業者が容易になし得る。

引用文献2では、顧客サービスセンターへの連絡を改めて加入者が行うことになっているが、発呼先を切り替える必要がある場合に、自動でルーティングする技術は引用文献3に示されており、引用文献2に引用文献3に記載された技術を適用することは当業者が容易になし得る。

拒絶の理由が新たに発見された場合には拒絶の理由が通知される。

引 用 文 献 等 一 覧

1. 国際公開第99/44387号パンフレット

2.特開平08-340331号公報

3.特開平 1 1 - 3 3 1 4 1 2 号公報

先行技術文献調査結果の記録

先行技術文献調査結果の記録

- ・調査した分野 I P C第7版 H 0 4 B 7 / 2 4 - 7 / 2 6
H 0 4 Q 7 / 0 0 - 7 / 3 8

H 0 4 Q 7 / 0 0 - 7 / 3 8

DB 名

- ・先行技術文献

この先行技術文献調査結果の記録は、拒絶理由を構成するものではない。